III. REMARKS

Claims 1-3 and 5-11 remain pending. Claims 1, 3 and 6 have been amended. Claim 4 has been canceled. Claims 12-37 have been withdrawn. Applicant does not acquiesce in the correctness of the rejections and reserves the right to present specific arguments regarding any rejected claims not specifically addressed. Further, Applicant reserves the right to pursue the full scope of the subject matter of the claims in a subsequent patent application that claims priority to the instant application.

Claims 1-11 have been rejected under 35 USC § 112 first paragraph, as failing to comply with the enablement requirement. Specifically, the Office objects to the term "tamper-proof". The Office has requested that this be changed to "tamper-resistant". Applicants have amended claims 1 and 6 accordingly.

Claims 1-11 have been rejected under 35 USC § 112 second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter of the invention. Specifically, the Office has objected to the term "computing environment" in claim 1, line 4. Claim 1 has been amended to claim a tamper-resistant secure data processing unit. It is believed this amendment overcomes the rejection in paragraph 13 of the Office Action. In paragraphs 16 and 17, claim 3 has been rejected as claiming a system and method. Applicants have amended claim 3 to replace "utilizes" with includes and to replace "process" with "program". Claim 4 has been canceled. In paragraph 18, claim 6 has been rejected for the recitation of "to be analyze future inputted transactions". Applicant has replaced this with "for analyzing future inputted transactions". It is believed that this amendment obviates the rejection of claim 6.

The Office has rejected claim 1 for the recitation of "secure data processing unit" (SDPU). The Office asserts this phrase is not lexicographically defined. The Office asserts that the description of the SDPU, found on page 3, paragraph 1, is not understood because it is not clear if two instances of each of "the security system", "analysis system", "plurality of surveillance algorithms" and "selection program" are required. Applicant fails to understand the Office's confusion as page 3, paragraph 1, provided below, recites:

"In a first aspect, the invention provides a system for detecting fraudulent transactions, comprising: an interface for inputting transaction data and outputting analysis results; and a secure data processing unit (SDPU) that provides a secret and tamperproof computing environment, wherein the SDPU includes: a security system that can restrict access to data and program execution; an analysis system for analyzing inputted transactions; a plurality of surveillance algorithms stored in an encrypted database; and a selection program for selecting at random times one or more different surveillance algorithms to be used by the analysis system."

Applicant asserts this language is clear. Furthermore, the Office is directed to Figs. 1 which clearly show the SDPU including a secure I/O system 18, a transaction analysis system 22, a library of encrypted surveillance programs 28 and an algorithm selection program 26. Fig. 2 also shows these elements. Applicant requests withdrawal of this rejection or a better explanation from the Office as to why the language and accompanying drawings are not clear.

The Office has rejected claims 3 and 4 under 35 USC § 101 because the claim is neither directed to a process nor a machine. Applicant has canceled claim 4 and claim 3 has been amended to recite a "random selection program", rather than "random selection process" obviating this rejection. Support for this amendment can be found on page 10, first paragraph, 3rd sentence and Fig. 1, item 26.

Claims 1, 2, 4-6, 8, 10 and 11 have been rejected under 35 USC § 103(a) as being unpatentable over Blumberg (US Pat. 6,240,415), hereinafter "Blumberg", in view of

Silverbrook et al. (US Pat. 6,317,192), hereinafter "Silverbrook". Applicant respectfully traverses this rejection.

The primary reference Blumberg is computerized management for an interactive system (Abstract). Remote users input their votes for management of a sports team. The votes are entered into the database and an algorithm processes votes for a decision and the most preferred choice is the one implemented (col. 10, line 20-col. 11, line 7). Exemplary Scenario 1 (col. 13, lines 8-22) has fans paying $1 for the right to participate in managing a team. The program uses inputs from the participants to determine salaries and bonuses (col. 13, lines 50-57). Blumberg does not teach elements of Applicant's claims as detailed below.

Applicant submits that Blumberg fails to show "a plurality of surveillance algorithms stored in an encrypted database; and a selection program for selecting at each of a sequence of random times a different surveillance algorithm to be used by the analysis system." The Office has cited col. 13, lines 37-49 in Blumberg as support for a plurality of surveillance algorithms. However, this passage in Blumberg explains that different algorithms and databases are used to establish probabilities and outcomes and consequences. Blumberg is using the input from the users and other statistical data to determine how a team is managed. These outcomes (salaries and bonuses) are based on the input of the fans or users (col. 13, lines 8-22). Thus, these algorithms are not surveillance algorithms as required by the claims of the instant invention. The surveillance algorithms of the present invention look at transactions and make some determination regarding the probability that the transaction is fraudulent (page 9, lines 8-11). In contrast, the algorithms of Blumberg take input data from users and output a result (Abstract). The result may be the micromanagement of a sports team in a league (col. 12, line 65- col. 13, line 5). The algorithms of Blumberg do not provide surveillance. Further, Blumberg does not

teach a selection program for selecting, at random times, a different surveillance program to monitor transactions. Blumberg (col. 9, lines 10-17) is cited by the Office to support a selection program, yet this passage teaches an operating system used to execute computer code and that the computer code can be stored on various devices. This passage of Blumberg does not provide any support for random selection surveillance algorithms. Thus, Blumberg fails to teach essential elements of the claimed invention and the rejection should be withdrawn.

Furthermore, the Office admits that Blumberg does not teach a tamper-resistant SDPU. The Office cites Silverbrook as teaching this feature. However, as explained above, Blumberg fails to teach the elements of "a plurality of surveillance algorithms stored in an encrypted database; and a selection program for selecting at each of a sequence of random times a different surveillance algorithm to be used by the analysis system." Thus, this combination is defective. Moreover, Silverbrook does not provide a tamper-resistant SDPU (claim 1) or a tamper resistant computing environment (claim 6). Silverbrook provides a method to ensure a message sent from party B to party A has not been intercepted. This is accomplished by a message authentication code generated by B and read by A. Combining this feature with Blumberg would not create a tamper resistant SDPU or a tamper resistant computing environment. Thus, the rejection should be withdrawn.

Claims 3 and 7-9 have been rejected under 35 USC § 103(a) as being unpatentable over Blumberg, in view of Silverbrook and further in view of Douceur et al. (US Pub. 2004/0060042), hereinafter "Douceur". Doeceur is cited by the Office to show a random selection and calculation of the correlation coefficient from the generated random values. The Office asserts that combining this with Blumberg and Silverbrook would yield Applicant's invention. Douceur does not correct the problem of the primary combination of Blumberg and Silverbrook.

Moreover, Douceur shows an algorithm to generate layouts wherein the algorithm has "random selection aspects" (page 4, paragraph [0050]). This algorithm than generates layouts of a program image that are compared based on a locality of reference (LOR) function (page 3, paragraph [0045]). Thus, Douceur teaches a single algorithm specific to image generation that has "random selection aspects". Applicant asserts that Douceur does not teach a selection program for randomly selecting surveillance algorithms. Therefore this combination does not provide a proper *prima facia* rejection of claim 2 and 7-9 and withdrawal is requested.

Applicant respectfully submits that the application is in condition for allowance. If the Examiner believes that anything further is necessary to place the application in condition for allowance, the Examiner is requested to contact Applicant's undersigned representative at the telephone number listed below.

Respectfully submitted,

/Carl F. Ruoff/

Dated: February 12, 2009

Carl F. Ruoff
Reg. No. 34,241

Hoffman Warnick LLC
75 State Street, 14th Floor
Albany, New York 12207
(518) 449-0044
(518) 449-0047 (fax)